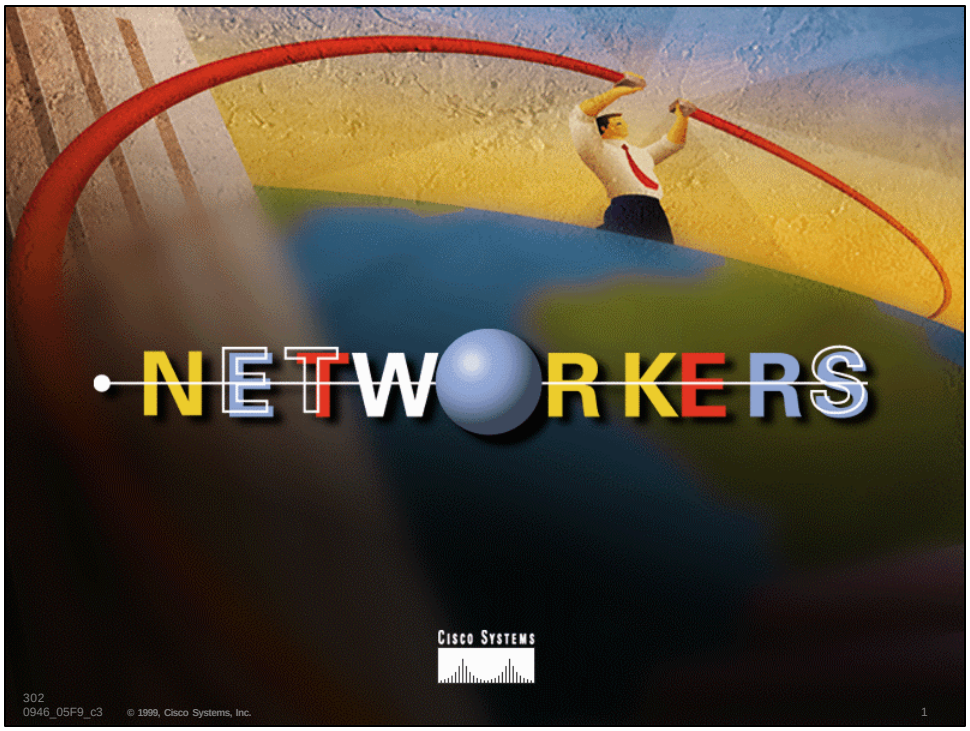
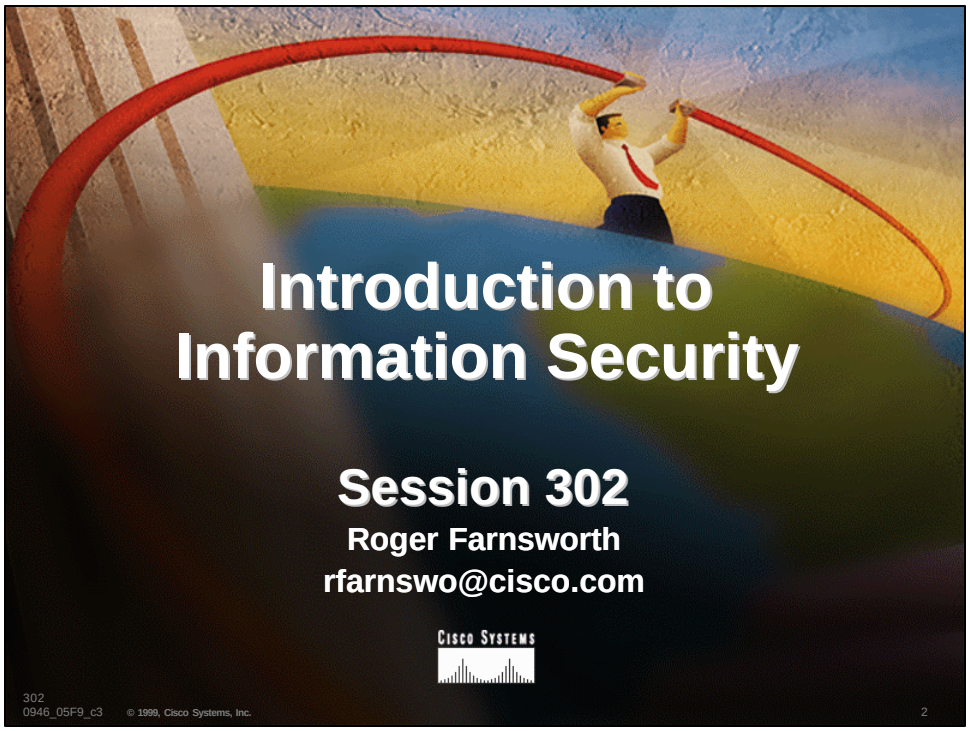
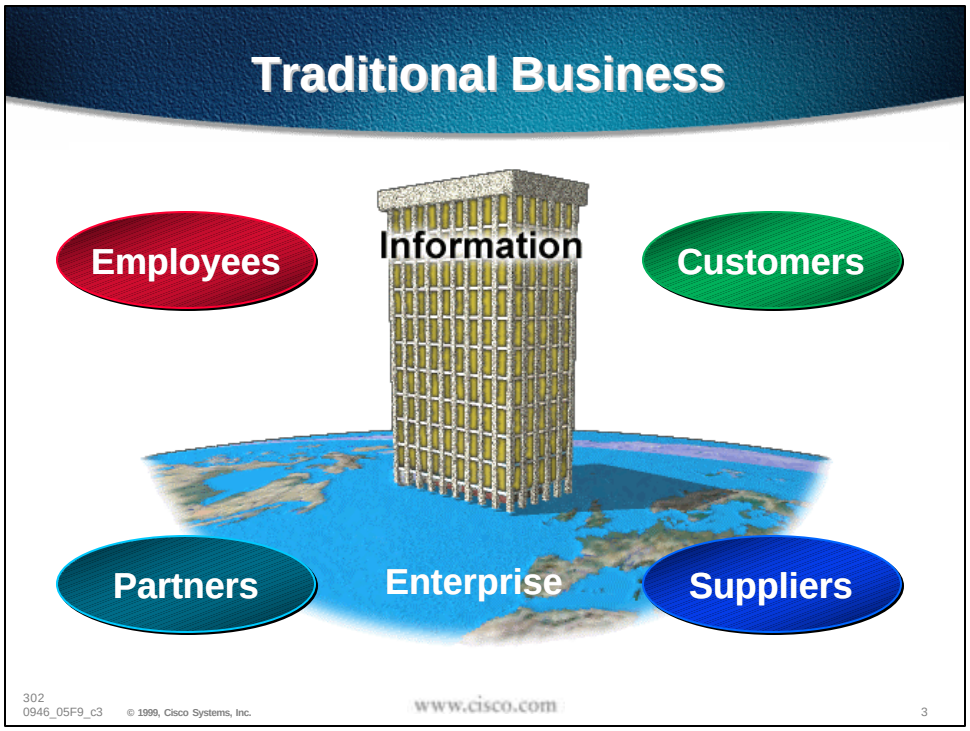
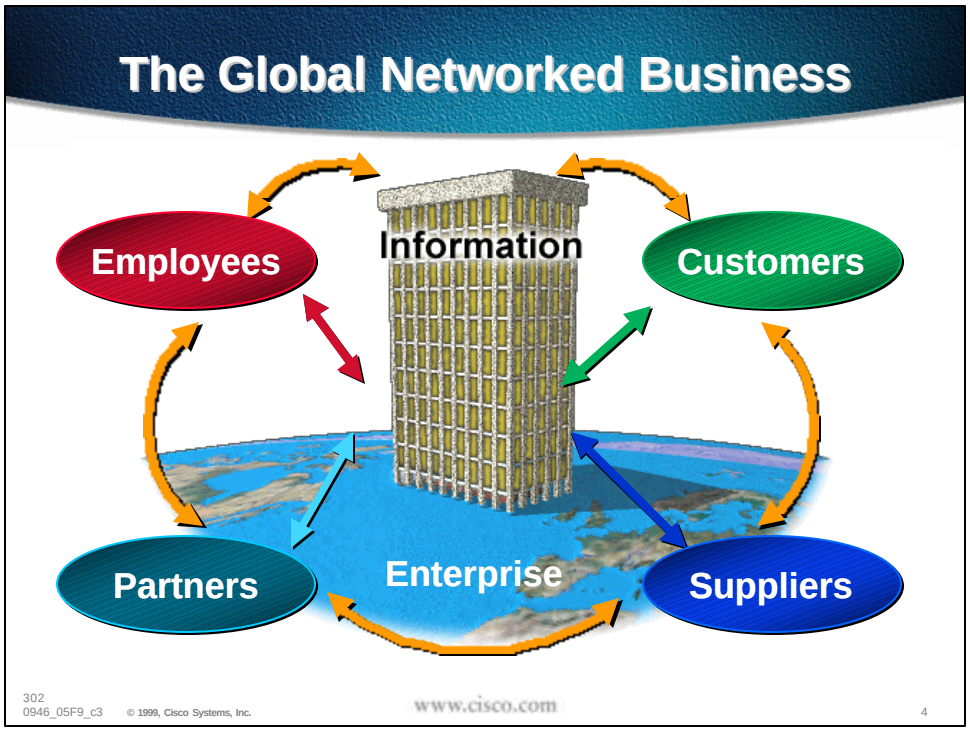
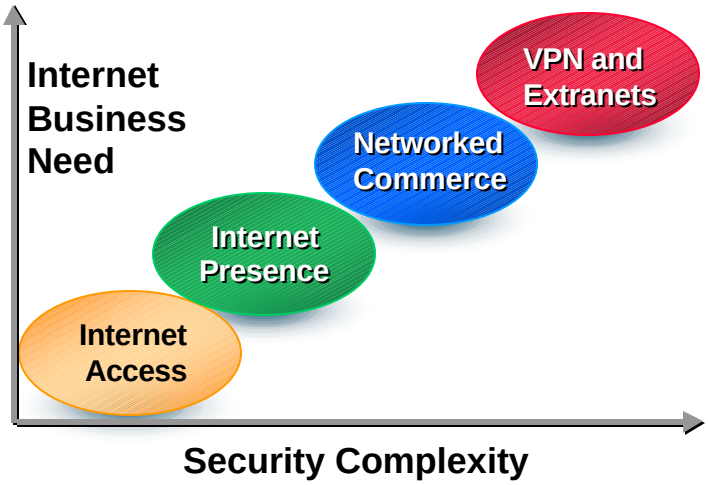




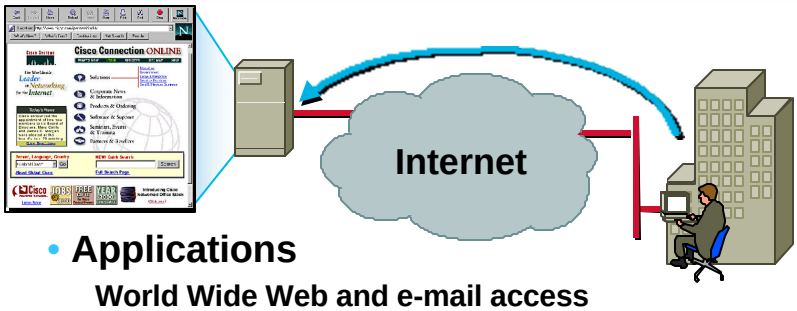




Business Problems?

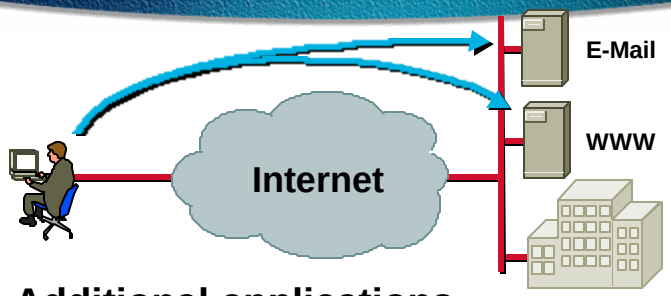


Enable Internet Access



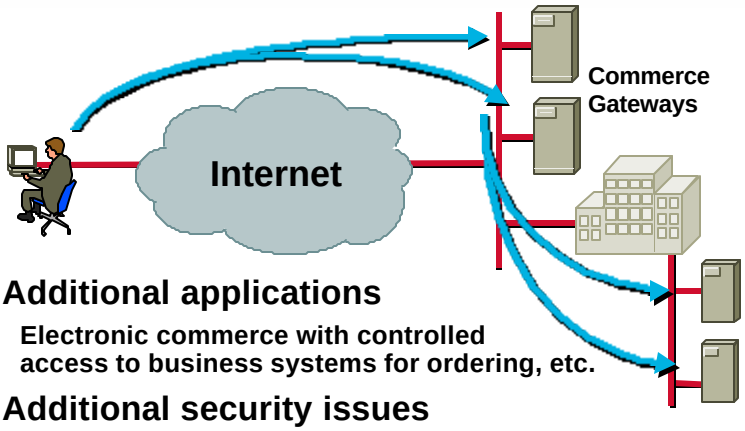
- **Applications**
  - World Wide Web and e-mail access
- **Security issues**
  - Protection of internal resources from outsiders
  - Limiting external privileges of internal users
  - Visibility of internal network addresses
  - Auditing usage and possible attacks

Enable Internet Presence



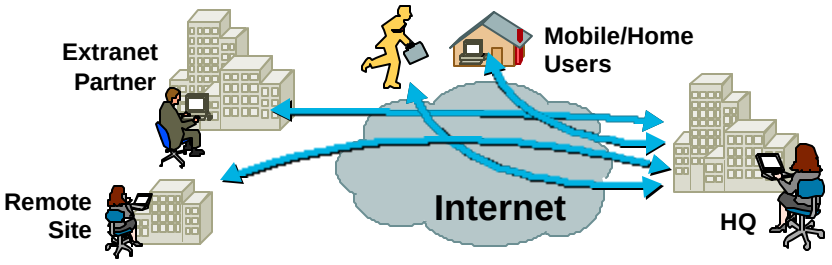
- **Additional applications**
  - E-mail server managed locally
  - Web server provides presence
- **Additional security issues**
  - Protection of public resources
  - Separation of public and internal networks

Enable Networked Commerce



- **Additional applications**
  - Electronic commerce with controlled access to business systems for ordering, etc.
- **Additional security issues**
  - Secure gateway-internal communication
  - Client-commerce gateway data privacy
  - Strong application authentication of client

Enable VPN and Extranets



- **Additional applications**
  - Private connections over public network
  - Virtual Private Network (VPN)
- **Additional security issues**
  - Encryption between remote users/sites and HQ
  - Strong network authentication of client

Why Security?

- **Three primary reasons**
  - Policy vulnerabilities
  - Configuration vulnerabilities
  - Technology vulnerabilities

And People Eager to Take Advantage of the Vulnerabilities

Security Objective: Balance Business Needs with Risks

Transparent Access

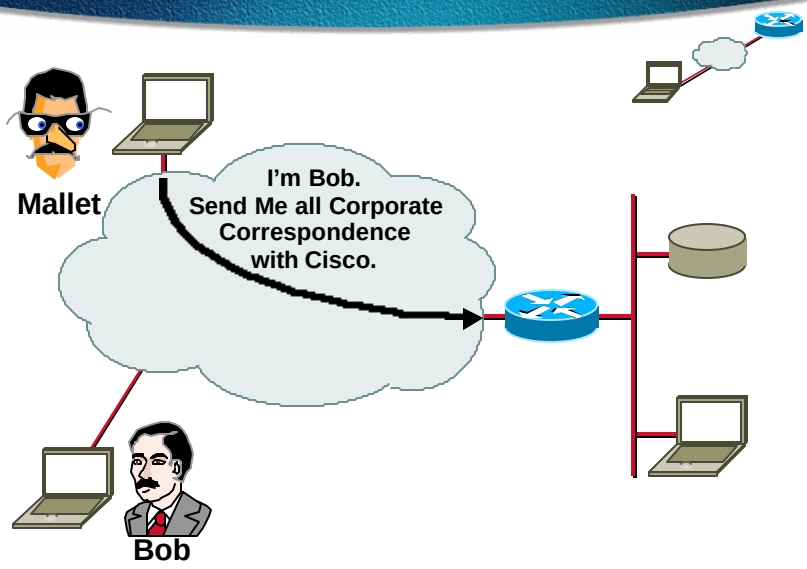
- Connectivity
- Performance
- Ease of Use
- Manageability
- Availability

Policy Management

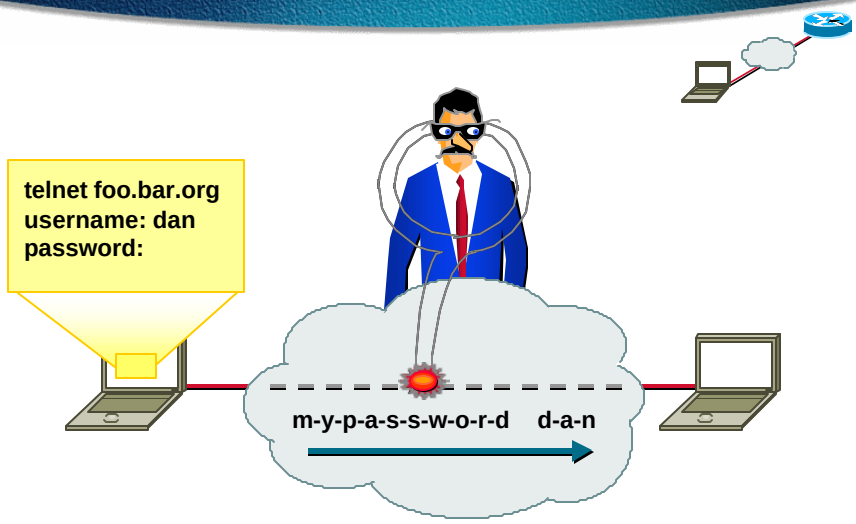
Security

- Authentication
- Authorization
- Accounting
- Assurance
- Confidentiality
- Data Integrity

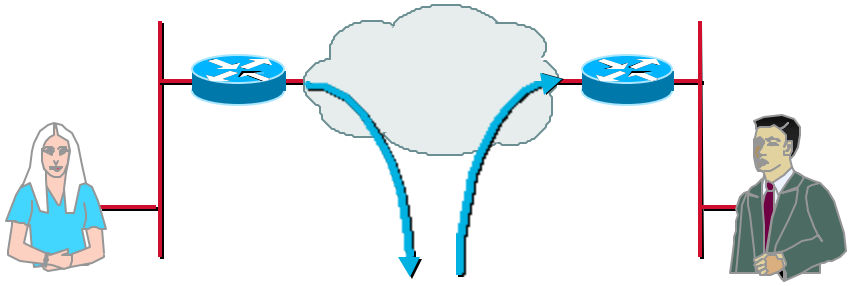
Threats: Identity Spoofing



Threats: Packet Sniffing



Threats: Data Theft

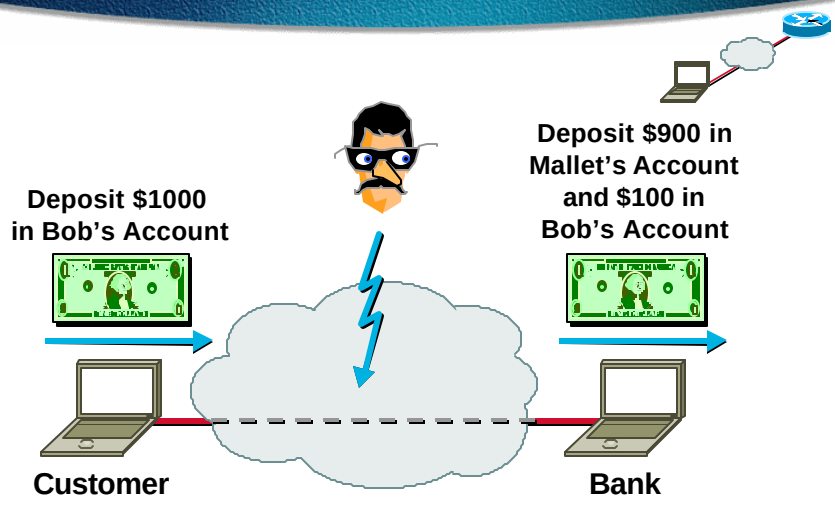


- **Corporate Business Plan:**

Expand into Mallet's core area

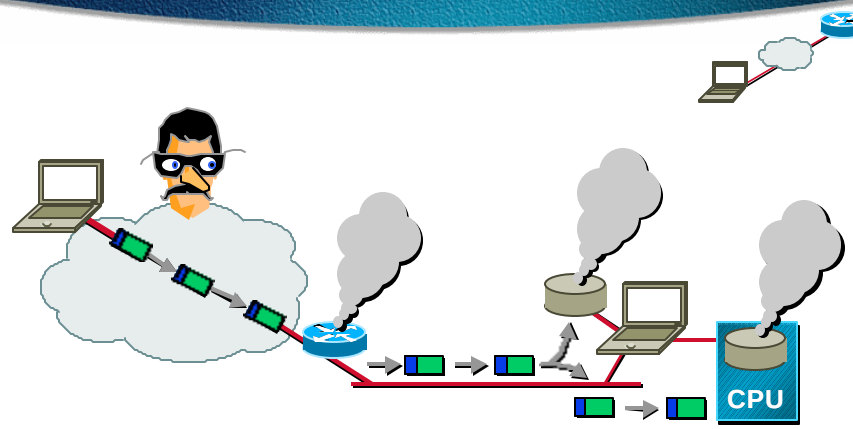
Massively discount our products for next quarter

Threats: Data Alteration



302
0946_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 15

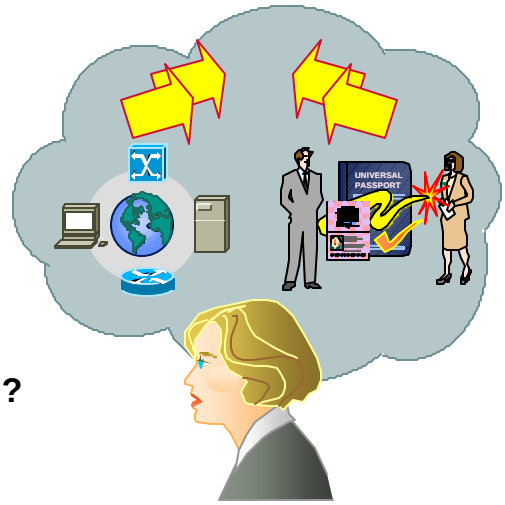
Threats: Denial of Service



302
0946_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 16

Policy—The Only Scalable Model

- **Enterprise-wide security policy**
  - **Who can see what information?**
  - **Who can change it?**
  - **From where?**
  - **How protected is it?**
  - **What are the assets ?**
  - **What is the cost ?**

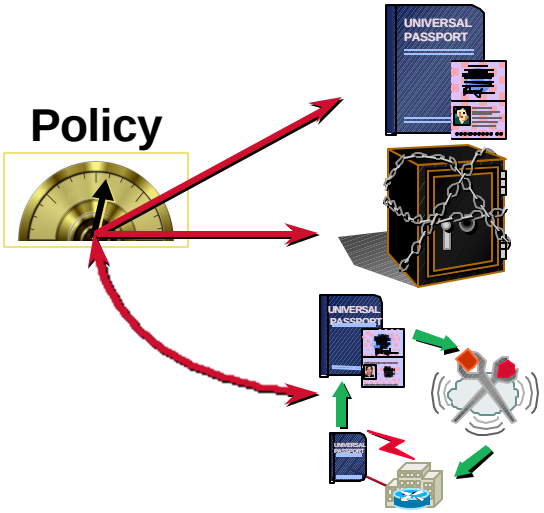


What Is a "Security Policy"?

"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."

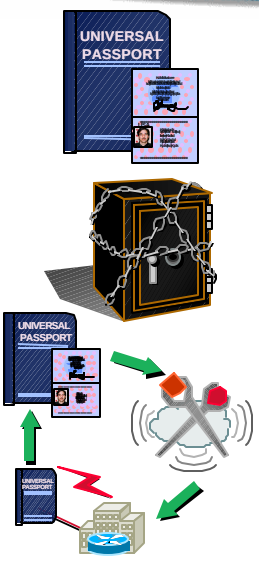
Source: RFC 2196,
Site Security Handbook draft

Cisco Enterprise Security Model



- Identity
- Integrity
- Active Audit

Security Technology Taxonomy



Identity

Accurately identify network users and their privileges

Integrity

Network integrity through:

- Secure network perimeters
- Privacy and encryption
- Reliable operation

Active Audit

Provide auditing, accounting and active detection and response

What Is the Appropriate Security Policy?

- **Open security policy**
  - Permit everything that is not expressly denied
- **Restrictive security policy**
  - Combination of specific permissions and specific restrictions
- **Closed security policy**
  - That which is not expressly permitted is denied

Setting Security Policies

- **Know your assets**
- **Count the costs**
- **Control secrets**
- **Allow for human factors**
- **Physical security**
- **Change management**

Identity

- Who are you?
- Where are you?
- What is permitted?

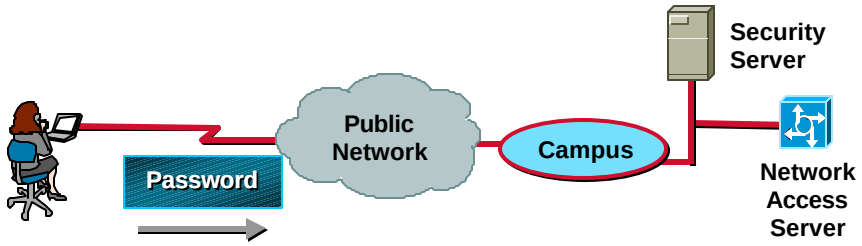
Methods of Authentication

Weak

- No username/password
- Static username/password
- Aging username/password
- One-Time Password (OTP)
  - S/Key—OTP for terminal login
  - PAP—OTP for PPP
- Token cards/soft tokens (OTP)
  - Enigma Logic, DES Card, Security Dynamics

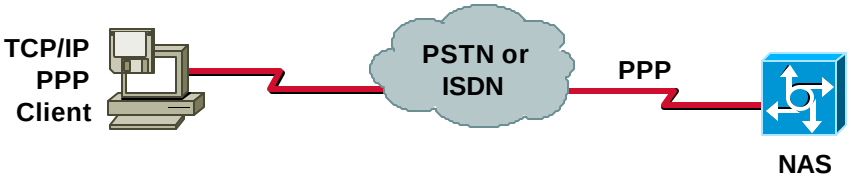
Strong

Username/Password



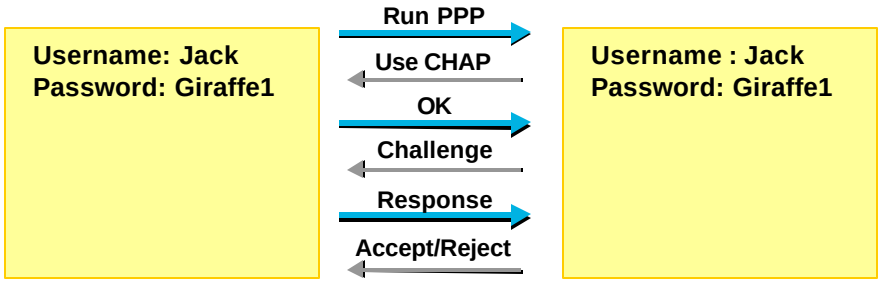
- Fundamental authentication mechanism
- Can be static or aging

PAP Authentication



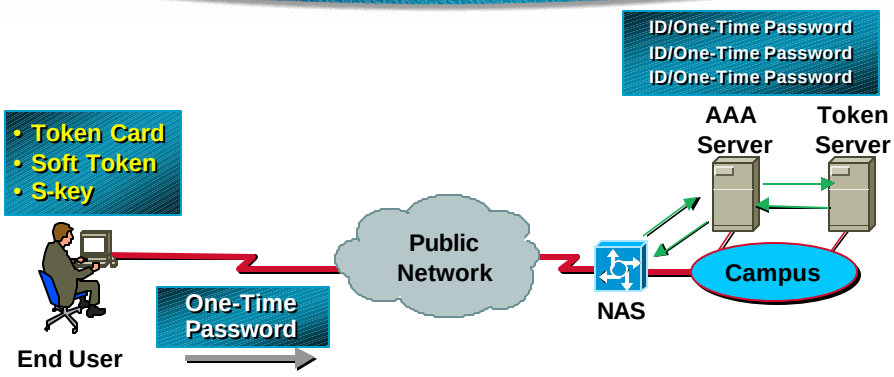
- PAP—Cleartext, repeated password
- NAS compares username/password to that stored in database, and accepts or rejects

CHAP Authentication



- Secret password per remote user
- "Three-way handshake" via challenge
- Product of (challenge* secret) provides authentication

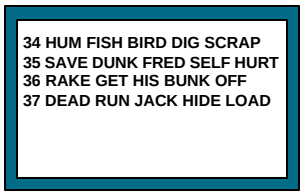
One-Time Passwords



- Password used one time only, sent in cleartext
- Can use token card or soft token, using algorithm based on PIN or time of day to generate secure password
- Token server uses same algorithm, sends password back to NAS to complete authentication

One-Time Passwords

- **S/KEY**
  - List of one-time passwords
- **Token cards**
  - Use algorithm based on PIN or time-of-day to generate passwords
  - Server uses same algorithm



Bio-Metrics

- **Finger-scan**
- **Face recognition**
- **Iris scan**

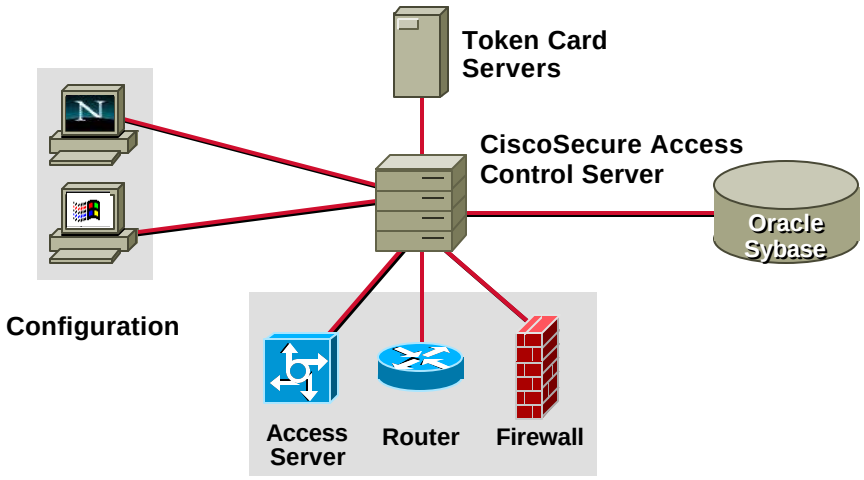
Authentication, Authorization and Accounting (AAA)

- Authentication = Verifies identity
  who are you?
- Authorization = Configures integrity
  what are you permitted to do?
- Accounting = Assists with audit
  what did you do?

Centralized Security Servers

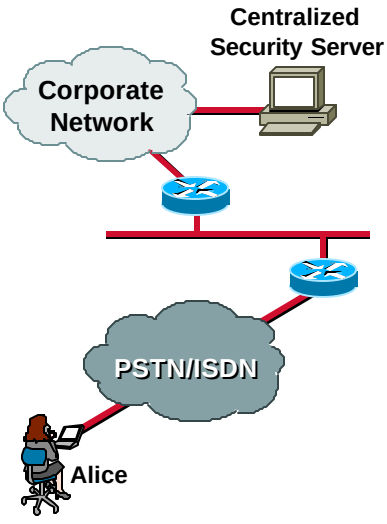
- Includes centralized security database with username, password and authorization information
- For use with a variety of authentication protocols including TACACS+, RADIUS, one-time password mechanisms

CiscoSecure: Identity for Dial, Internet, and Campus

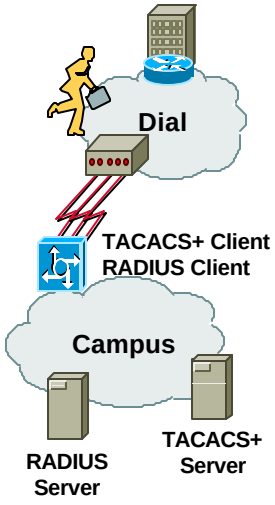


Centralized Security (AAA) Server

- Can be based on TACACS+ or RADIUS protocols
- Maintains database of user information
- Authenticates dial-in users
- Downloads user authorization information to NAS
- If user information changes, network administrator only has to change information on centralized server

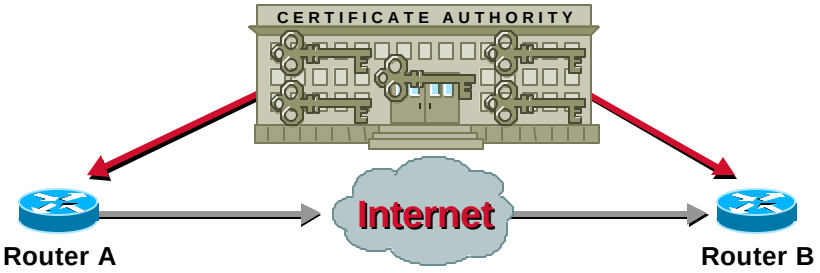


TACACS+/RADIUS Comparison



	TACACS+	RADIUS
Functionality	Separates AAA	Combines Authentication and Authorization
Transport Protocol	TCP	UDP
Authentication	Bi-Directional	Uni-Directional
Protocol Support	Full Support	No ARA No NetBEUI
Confidentiality	Entire Packet-Encrypted	Password-Encrypted

Device Authentication



- Certificate Authority (CA) verifies identity
- CA signs digital certificate containing device's public key
- Certificate equivalent to an ID card

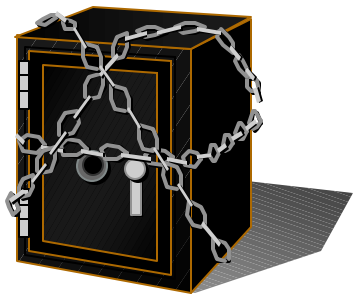
Digital Certificates

- **A digital certificate contains:**
  - **Serial number of the certificate**
  - **Issuer algorithm information**
  - **Valid to/from date**
  - **User public key information**
  - **Signature of issuing authority**

0000123
SHA,DH, 3837829....
1/1/93 to 12/31/98
Alice Smith, Acme Corporation
DH, 3813710...
Acme Corporation, Security Dept.
SHA,DH, 2393702347 ...

Integrity

- **Physical security**
- **Maintain data confidentiality**
- **Secure perimeters**
- **Secure communications**



0946_05F9_c3.scr

Physical Security

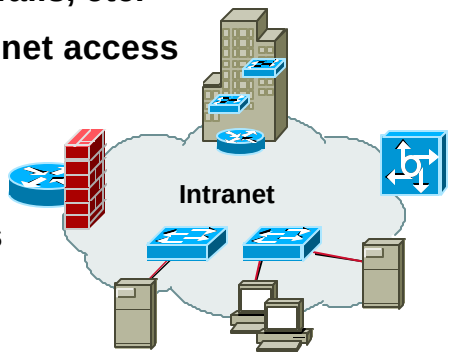
Small Equipment Is Easy to Hide

Large Equipment Is Too Heavy to Lift

Reality Check—Lock Equipment Racks and Doors!

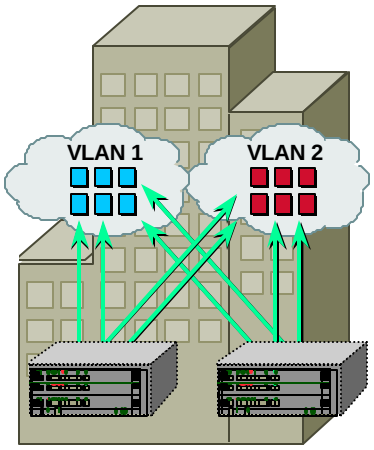
Secure Configurations for All Infrastructure Components

- Routers, switches, firewalls, etc.
- Secure console and Telnet access
  - Simple clear-text password by default
  - TACACS+ or RADIUS
- Multiple privilege levels for configuration and user commands
- Encrypted passwords when viewing configurations



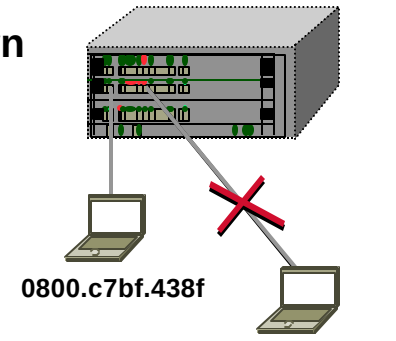
Workgroup Security: VLANs

- Isolates protected clients by:
  - Switch port
  - MAC address
  - Network address
  - Application type
- Inter-VLAN controls via Cisco IOS™ access controls



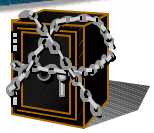
Workgroup Port Security

- MAC address lockdown
- Static or first learned address
- Port is disabled after unsecured address is seen and initiates link-down trap with port security flag

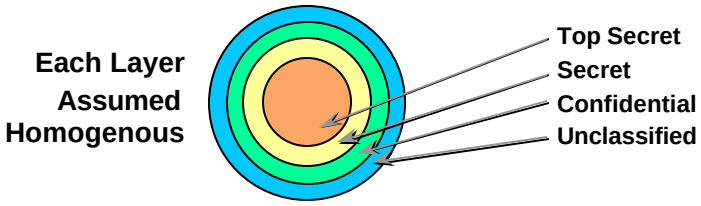


(Learned Address Was: 0800.c7bf.1234)

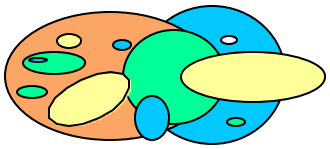
Perimeter Controls



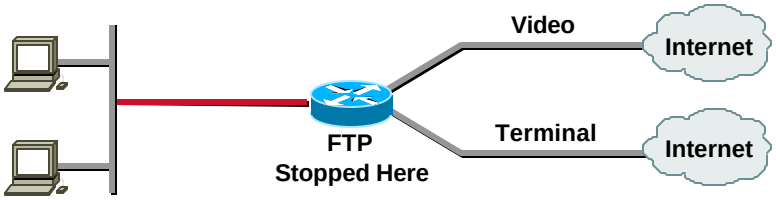
- Firewalls focuses on us and them



- Most networks are more like this:

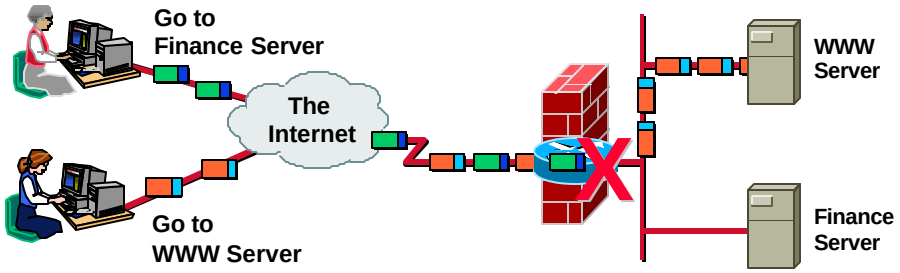


Policy Enforcement Using Access Control Lists



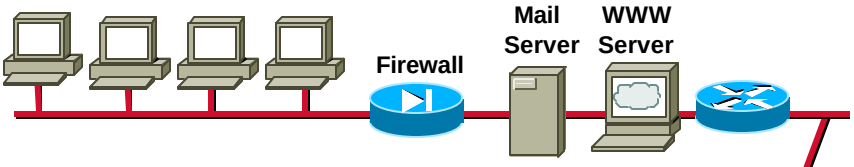
- Ability to stop or reroute traffic based on packet characteristics
- Access control on incoming or outgoing interfaces
- Works together with NetFlow to provide high-speed enforcement in campus networks
- Violation logging provides useful information to network managers

Packet Filtering Firewall

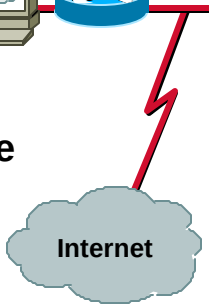


- Most versatile for adding protocols and new applications
- Less conducive to authentication and authorization
- Minimal auditing functions for user sessions

Stateful Packet Filtering



- More stringent security
- Maintains complete session state
- Connection oriented
  - Tracks complete connection
  - Establishment and termination
- Sessions immune to hijacking
- Strong audit capability



Cisco PIX™ Firewall

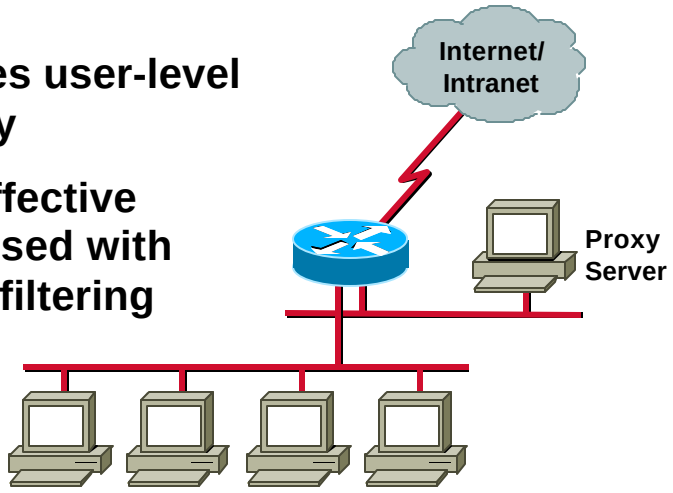
- Dedicated firewall appliance
- Strong security
  - ITSEC E1 Certified
- Highest performance on the market
  - 16,000 sessions
  - 90 Mbps throughput
- Simple setup

What Is an Appliance?

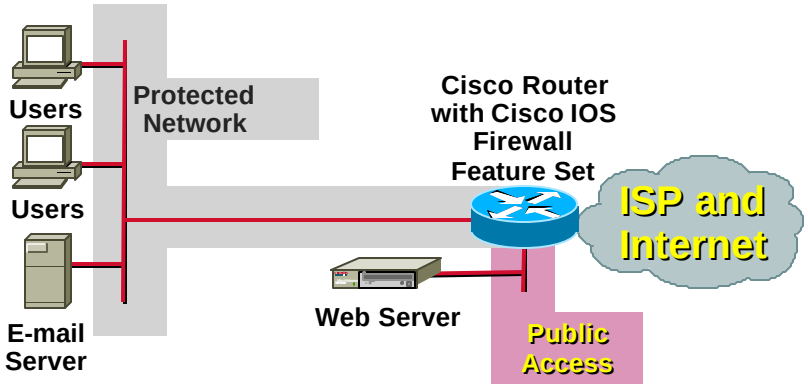
- Equipment dedicated to just one job
- Easy to install and use
- Very reliable

Proxy Service

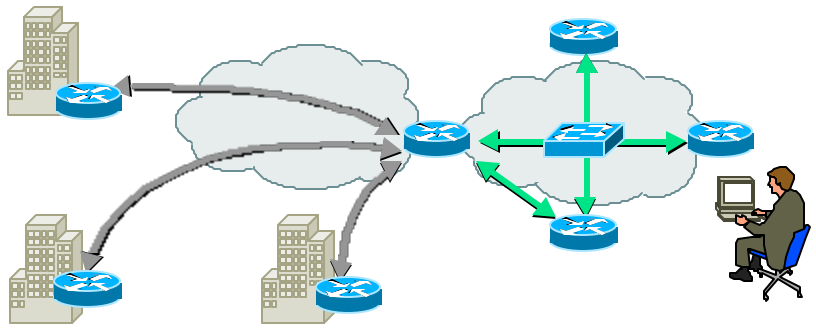
- Provides user-level security
- Most effective when used with packet filtering



Securing Network Perimeter and DMZ IOS Firewall Feature Set



Business Drivers of Data Confidentiality



- Extend the corporate network across the Internet
- Conduct business over the Internet
- Reduce remote access costs

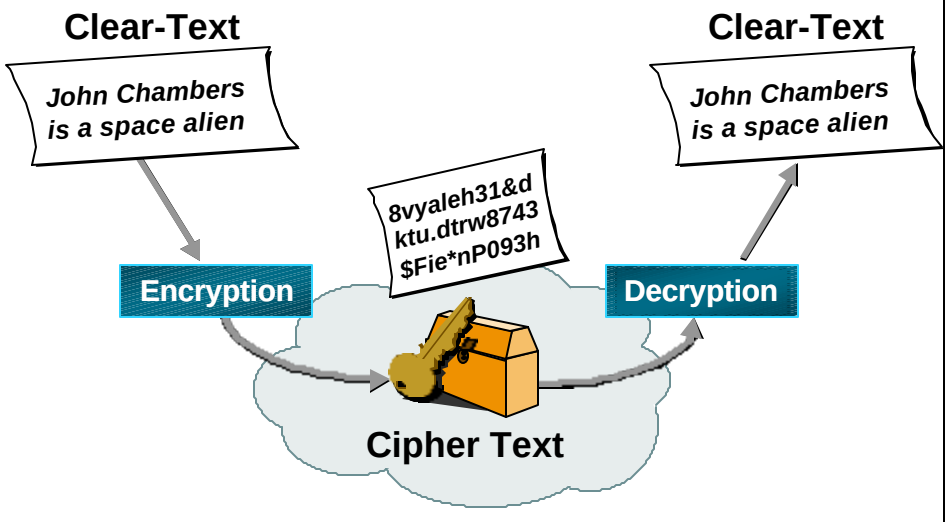
Challenges of Data Confidentiality

- Protect confidentiality of data over an untrusted network
- Ensure identity of users and systems
- Scale from small to very-large networks
- Implement a manageable key exchange system

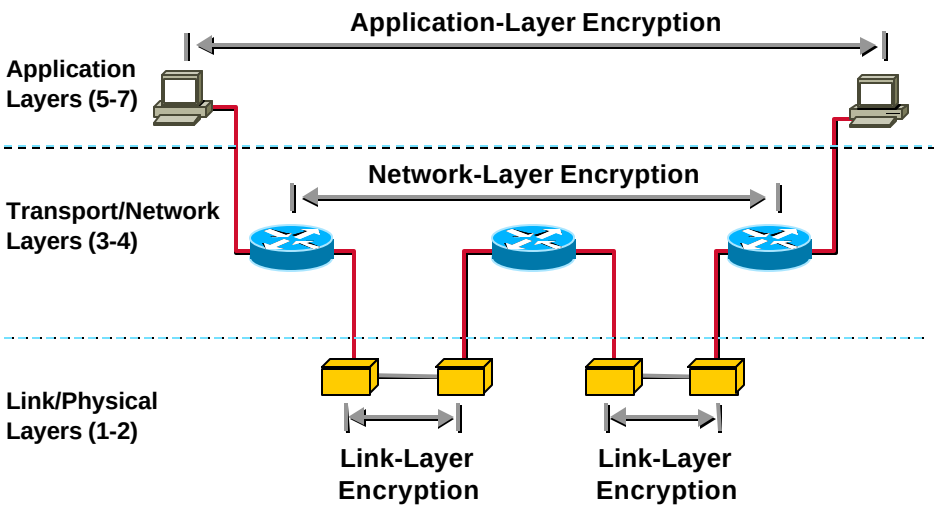
Cryptography

- Cryptographic technologies can provide:
  - Authentication
  - Confidentiality
  - Integrity
- Network infrastructure
  - Routing updates, management
- Secure user-data transport

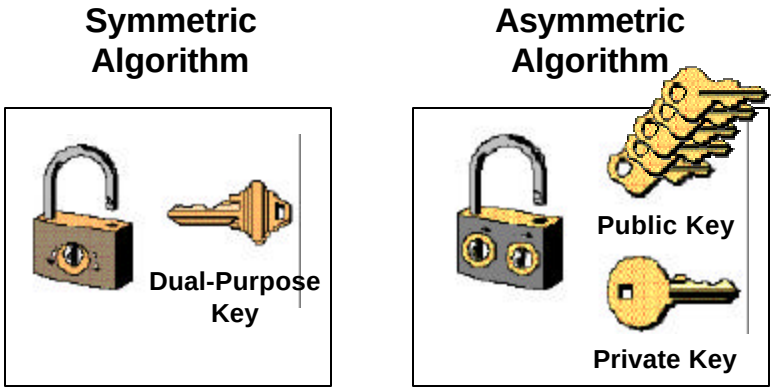
Encryption and Decryption



Encryption Alternatives



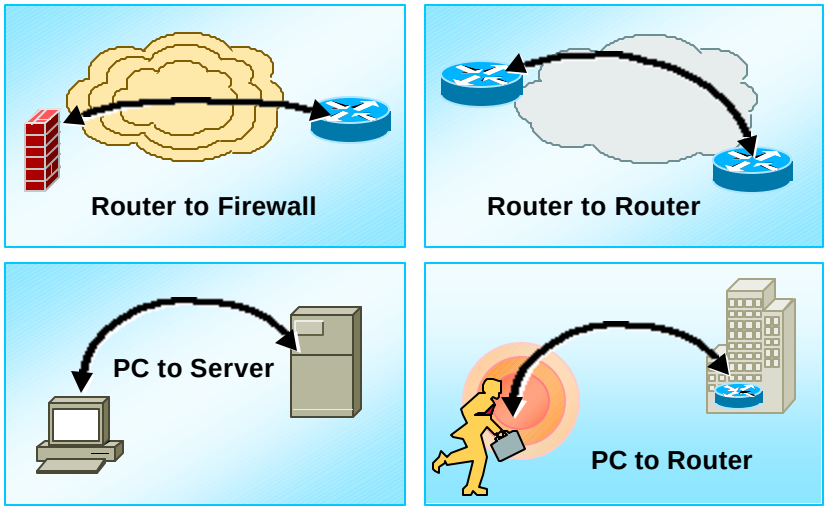
Classical Cryptography vs. Public Key



What Is IPSec?

- Network-layer encryption and authentication
- Open standards for ensuring secure, private communications over any IP network, including the Internet
- Provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy
- Data protected with network encryption, digital certification, and device authentication

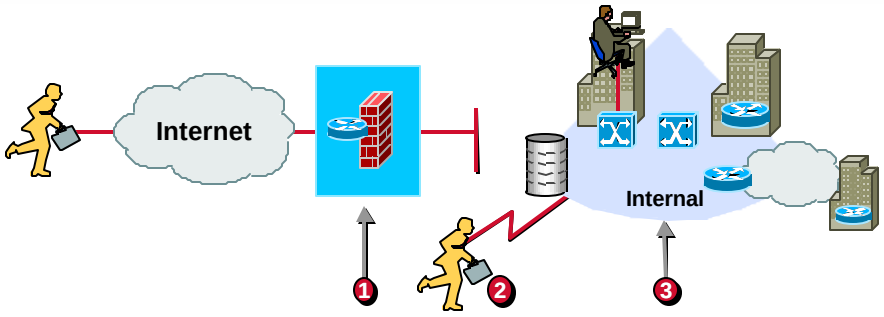
IPSec Everywhere!



Benefits of IPSec

- Privacy, integrity and authenticity for networked commerce
- Implemented transparently in the network infrastructure
- End-to-end security solution including routers, firewalls, PCs and servers

Open Design



1. Firewall

FW/Router with Access Lists, No Per-User Identity, No Data Encryption

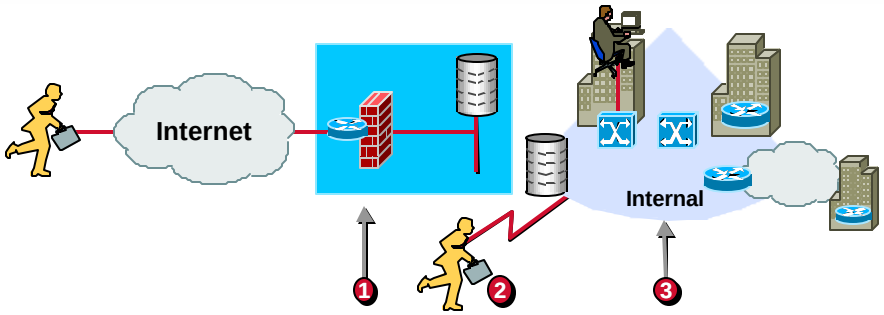
2. Dial

Identity Is Password Authentication—Pap or Chap to CiscoSecure™

3. Internal

Passwords for Telnet and Console Access Equipment, No Data Encryption

Restrictive Design Example



1. Firewall

Separate Gateway Router and Dedicated Stateful Firewall (Cisco IOS Router and PIX)

2. Dial

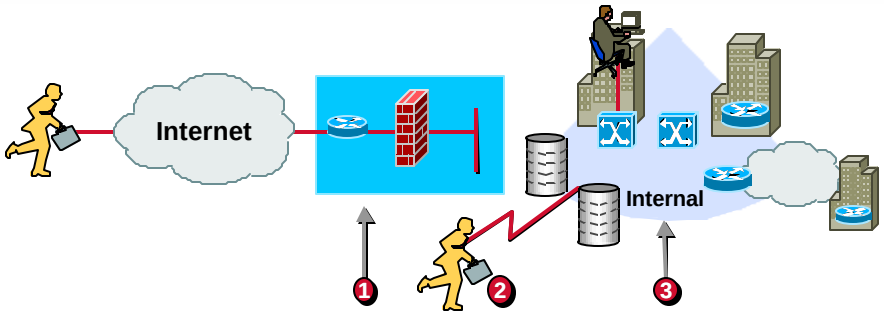
Identity Is Password Authentication—Pap or Chap to CiscoSecure™

3. Internal

Equipment Configuration and Access CiscoSecure Passwords and Privilege Levels, Route Authentication, VLANs

Encryption to Branches (Cisco IOS 11.2)

Closed Design Example



1. Firewall

Separate Gateway Router and Dedicated Stateful Firewall (Cisco IOS Router and PIX) Identity using PIX and CiscoSecure

2. Dial

Digital Certificate Authentication, use Encryption (Available with IPsec Implementation—Cisco IOS 12.0?)

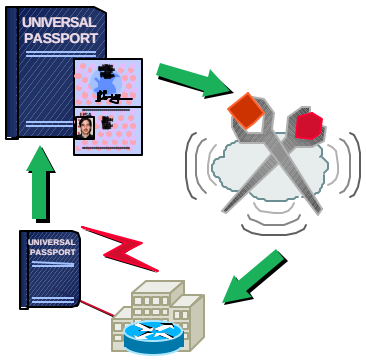
3. Internal

Equipment Configuration and Access w/CA and Privilege Levels

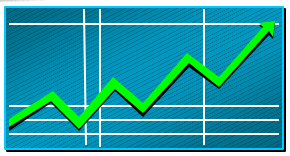
Encryption between All WAN Routers (Cisco IOS 11.2)

Active Audit

- Verify policy
- Assurance
- Reporting
  - Attacks
  - Errors
  - Misuse
  - Anomalies



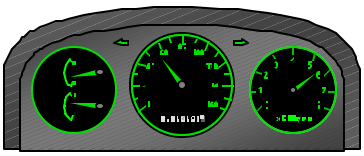
Monitor the Network



- The monitoring system

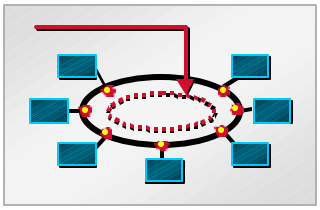
  Based upon your business goals, what will you measure and report?

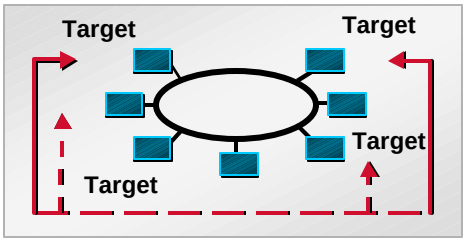
  Need to validate that the connection is meeting your business goals



Cisco NetSonar Vulnerability Scanning

- **Network Mapping**
  - Identify live hosts
  - Identify services on hosts
- **Vulnerability Scanning**
  - Analyze discovery data for potential vulnerabilities
  - Confirm vulnerabilities on targeted hosts



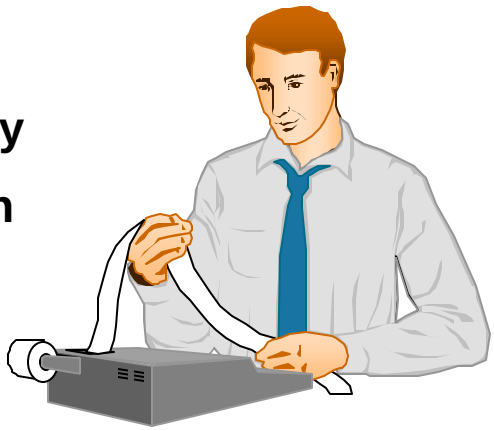


Cisco NetRanger

- **Sensors watch for attacks or problems**
- **NetRanger stops active attacks**

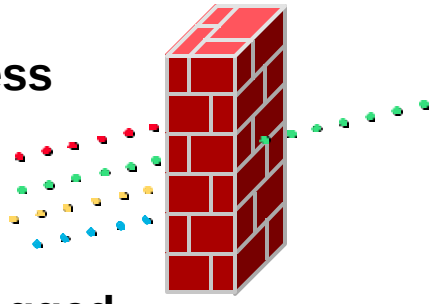
Accounting/Logging

- Actively audit and verify policy
- Detect intrusion and anomalies
- Report



Monitoring

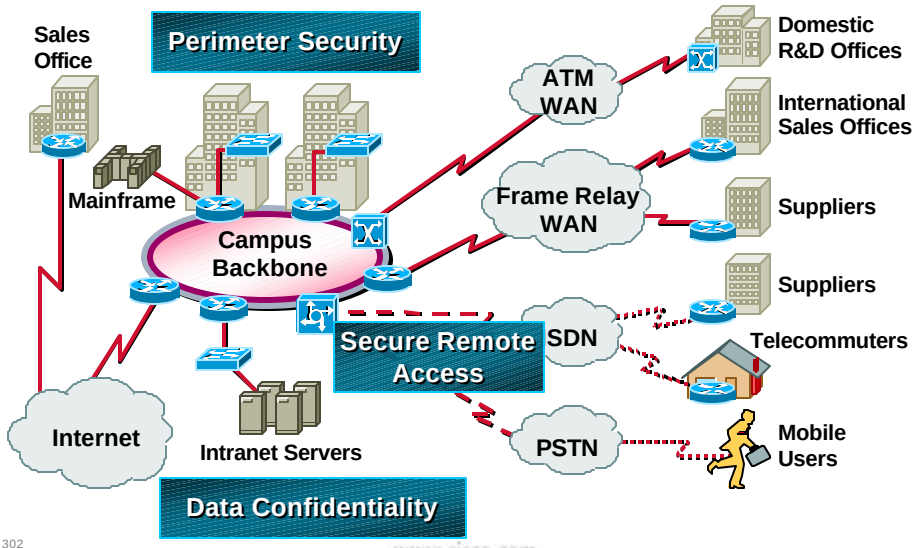
- Inbound and outbound traffic
- Source and destination address
- Port number
- Implicit denial
- Illegal attempts logged



Cisco Security Products (and Where They Fit)

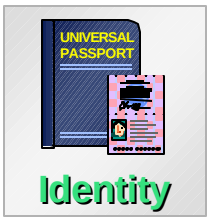
- **Identity**
  - CiscoSecure ACS family
- **Integrity**
  - **Firewalls:**
    - PIX firewall
    - Cisco IOS firewall feature set
    - Cisco IOS security features
- **Integrity**
  - Network-layer encryption
  - IPSec
- **Audit**
  - NetSonar™
  - NetRanger™
  - NETSYS™

Cisco End-to-End Network Security Services



Conclusions

- Have a written security policy
- Balance ease-of-use with security
- Security touches every element of the IT infrastructure; it is pervasive
- The core elements of network security are:



- Security applies to active network equipment as well as the application data

More Info at Networkers...

Deploying Security Technology	Wednesday 2-4	Thursday 10-12
Advanced Security Technology Concepts	Thursday 2-4	Friday 9-11
Introduction to Cisco Security Manager	Thursday 4-5	
Deploying VPNs and Tunneling Technology	Wednesday 12-2	Thursday 12-2
Intrusion Detection and Scanning with Active Audit	Thursday 3-4	
New Developments for the Enterprise Virtual Private Network	Friday 10-11	
Update on Firewall Technologies	Thursday 2-3	

More Info at Networkers…

Introduction to VPNs and Tunneling	Wednesday 11-12	Thursday 11-12
Cisco Security Consulting Services Update	Thursday 12-1	
Extranet Architecture	Wednesday 12-2	Wednesday 2-4
Security Birds-of-a-Feather	Wednesday 6-7	

Questions?